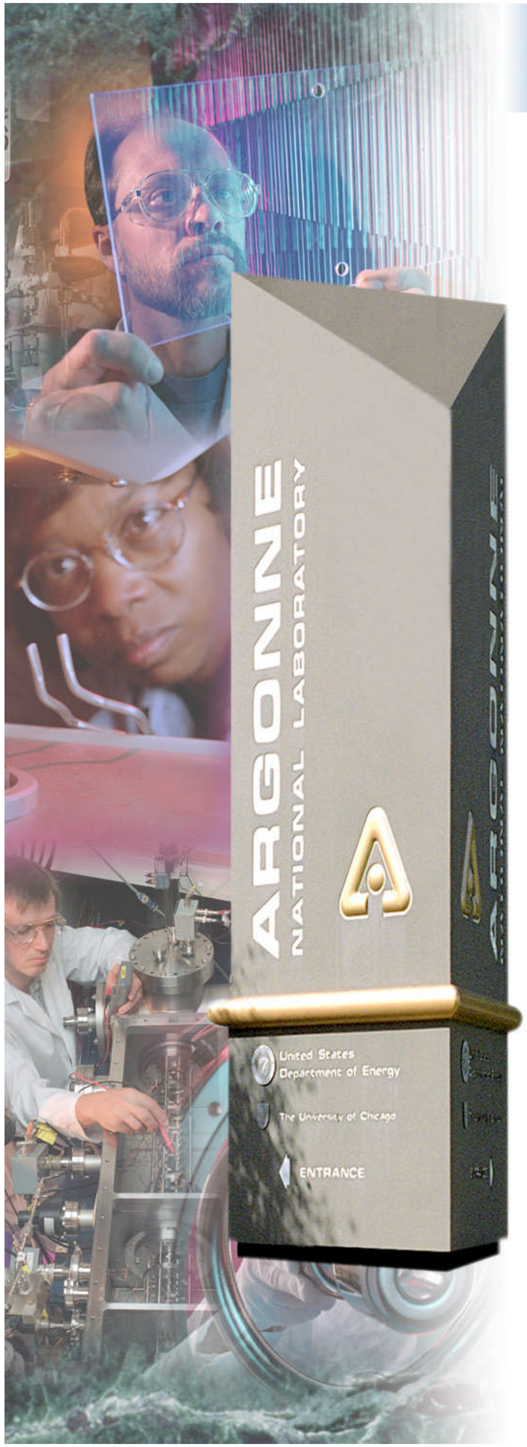
ARGONNE NATIONAL LABORATORY



APS Networking

Dave Leibfritz

December 13, 2005

THE UNIVERSITY OF CHICAGO

Office of Science
U.S. DEPARTMENT OF ENERGY

Argonne National Laboratory is managed by
The University of Chicago for the U.S. Department of Energy

APS Network Infrastructure

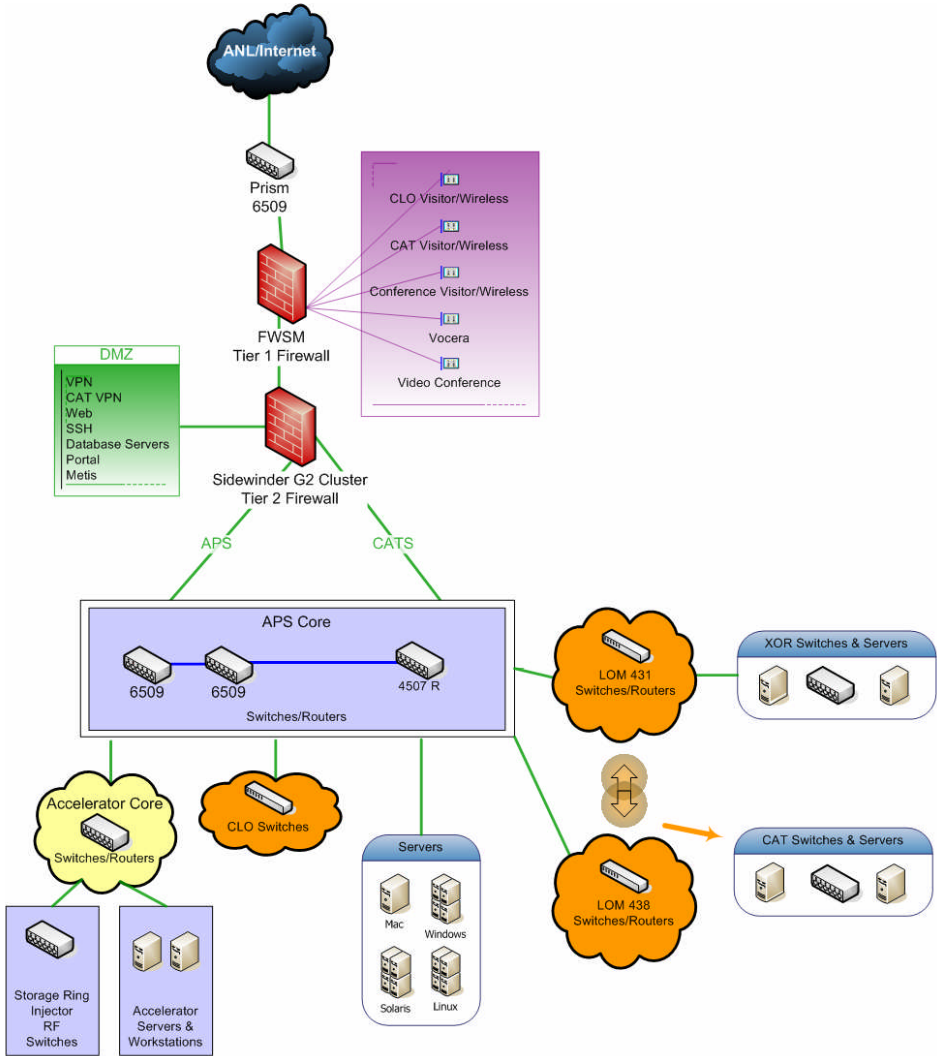
- IT designs, installs and maintains the network for APS including:
  - Accelerator network: Storage Ring, Injector and RF
  - 400 EAA
  - 401 CLO
  - 402 Conference Center
  - LOMs 431 – 438
  - 460 AGH
  - Bldg 300 area
  - Bldg 450
  - Wireless Service

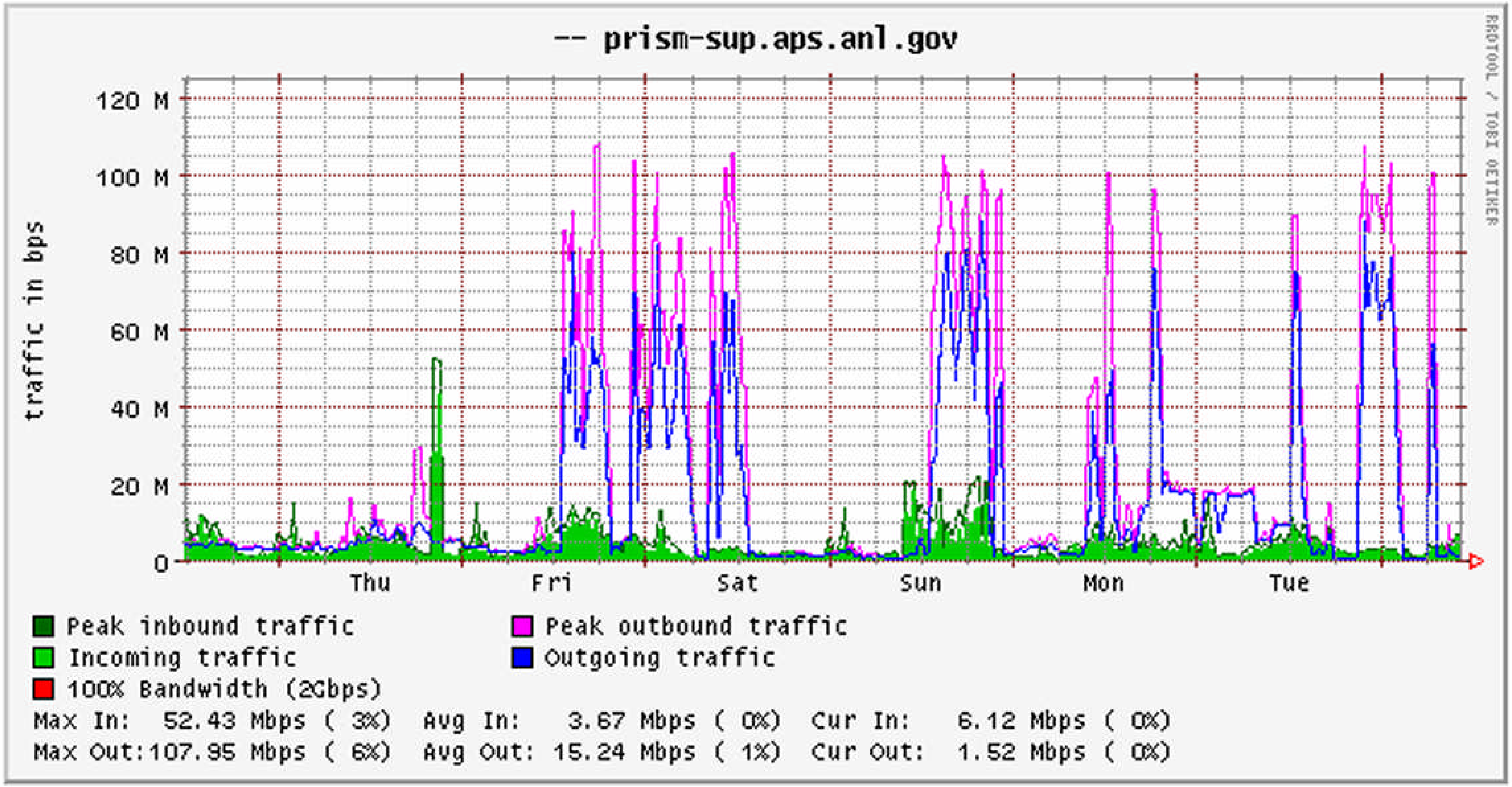
APS Network Infrastructure continued

- APS - 4500 nodes
  - 45 switches/routers
  - 20 subnets

- Beamlines - 4200 nodes
  - 20 switches/routers
  - 55 subnets

APS Network


ANL/Internet
Prism
6509
CLO Visitor/Wireless
CAT Visitor/Wireless
Conference Visitor/Wireless
Vocera
Video Conference
FWSM
Tier 1 Firewall
DMZ
VPN
CAT VPN
Web
SSH
Database Servers
Portal
Metis
Sidewinder G2 Cluster
Tier 2 Firewall
APS
CATS
APS Core
6509
6509
4507 R
Switches/Routers
LOM 431
Switches/Routers
XOR Switches & Servers
CAT Switches & Servers
LOM 438
Switches/Routers
Accelerator Core
Switches/Routers
CLO Switches
Servers
Mac
Windows
Solaris
Linux
Storage Ring
Injector
RF
Switches
Accelerator
Servers &
Workstations



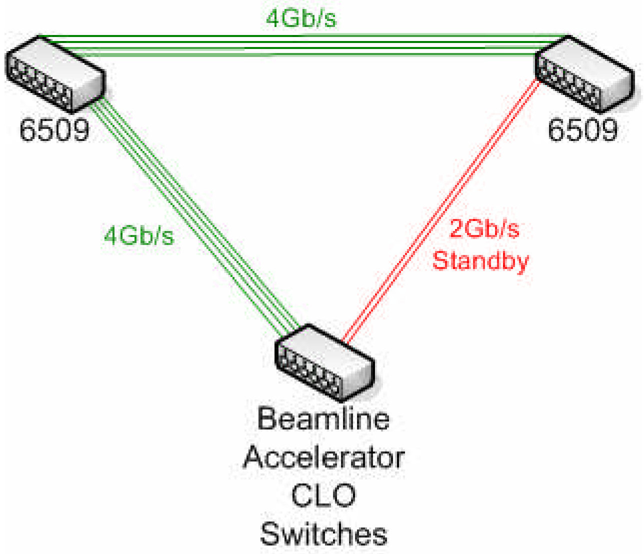
```
Max In:   52.43 Mbps ( 3%)  Avg In:    3.67 Mbps ( 0%)  Cur In:    6.12 Mbps ( 0%)
Max Out:107.95 Mbps ( 6%)  Avg Out:  15.24 Mbps ( 1%)  Cur Out:   1.52 Mbps ( 0%)
```

Last update: Wed Oct 12 10:16:07 2005

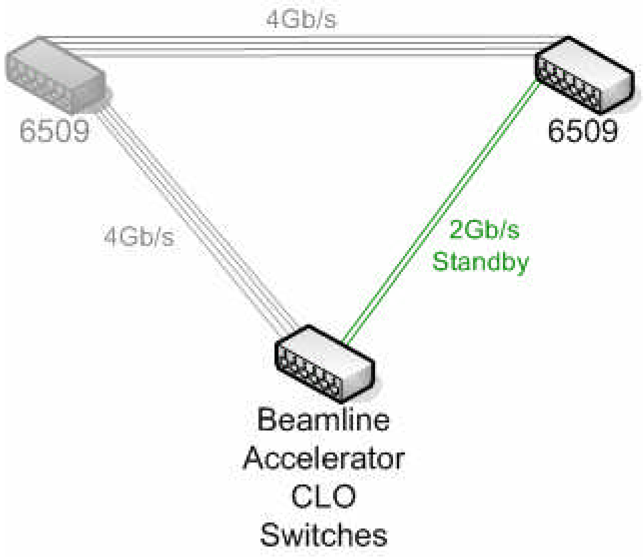
APS Network Switches

- Cisco's switches/routers set standard for high-end LAN switching
  - High Availability/Redundancy - stateful switchover
  - Hot swappable modular components - in house spares
  - Firmware upgrades - almost no downtime
  - Online diagnostics
  - IT scripts provide daily port error reports - Irmis
  - Same management tools for all Cisco switches
  - Follow Best Practices from Cisco

Network Redundancy



Network Redundancy



Wireless Access Points

CLO	28
Beamlines	56
Conference Areas	6
Guest House	12
TOTAL	**102**

Wireless Speed Capabilities

- All Access Points support 802.11b and 802.11g wireless clients

802.11b

- Supports older wireless clients
- Speeds up to 11 Mbps

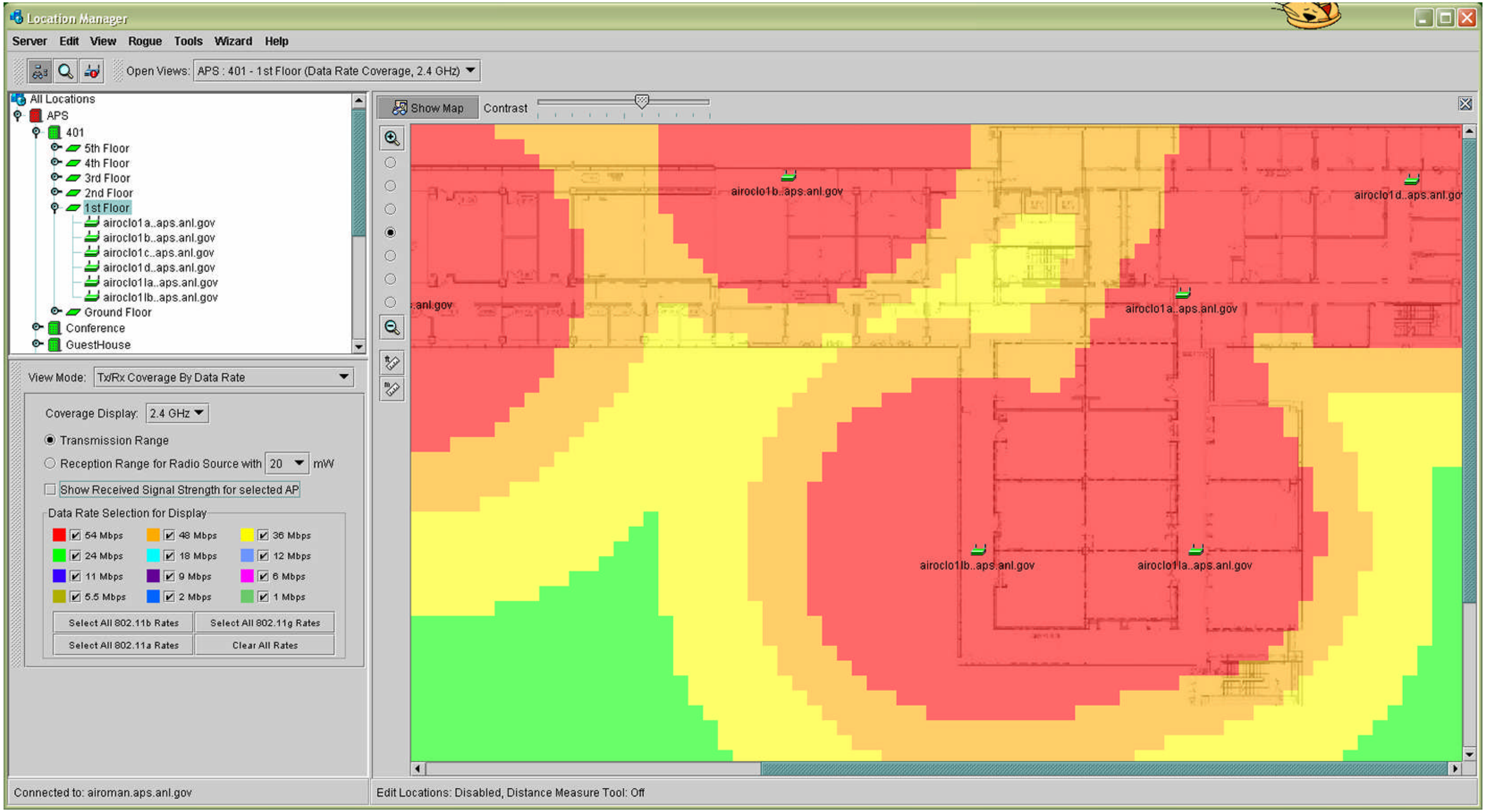
802.11g

- Standard on new laptops
- Speeds up to 54 Mbps

Cisco Wireless LAN Solution Engine

- The CiscoWorks WLSE is a centralized, systems-level application for managing and controlling an entire Wireless LAN infrastructure.

- Offers centralized management of wireless access points
- Detects, locates and mitigates rogue access points
- Monitors performance and faults
- Detects RF interference
- Automatically optimizes radio coverage and settings
- Self healing



Open Views: APS : 401 - 1st Floor (Data Rate Coverage, 2.4 GHz)

- All Locations
  - APS
    - 401
      - 5th Floor
      - 4th Floor
      - 3rd Floor
      - 2nd Floor
      - 1st Floor
        - airoclo1a..aps.anl.gov
        - airoclo1b..aps.anl.gov
        - airoclo1c..aps.anl.gov
        - airoclo1d..aps.anl.gov
        - airoclo1la..aps.anl.gov
        - airoclo1lb..aps.anl.gov
      - Ground Floor
    - Conference
    - GuestHouse

View Mode: Tx/Rx Coverage By Data Rate

Coverage Display: 2.4 GHz

● Transmission Range

○ Reception Range for Radio Source with 20 mW

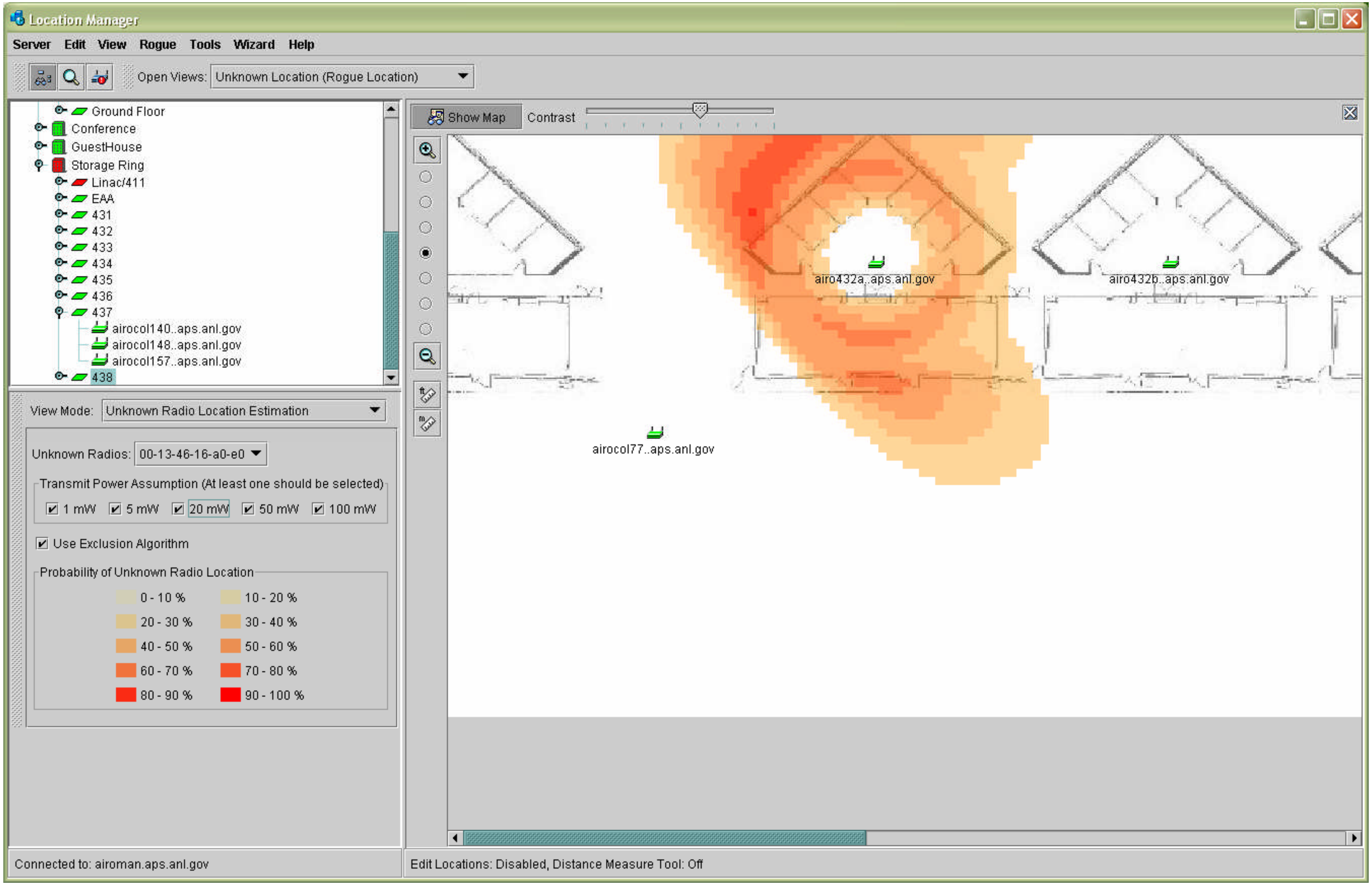
□ Show Received Signal Strength for selected AP

Data Rate Selection for Display

🟥 ☑ 54 Mbps	🟧 ☑ 48 Mbps	🟨 ☑ 36 Mbps
🟩 ☑ 24 Mbps	🟦 ☑ 18 Mbps	🟦 ☑ 12 Mbps
🟦 ☑ 11 Mbps	🟪 ☑ 9 Mbps	🟪 ☑ 6 Mbps
🟫 ☑ 5.5 Mbps	🟦 ☑ 2 Mbps	🟩 ☑ 1 Mbps

Connected to: airoman.aps.anl.gov

Edit Locations: Disabled, Distance Measure Tool: Off



Open Views: Unknown Location (Rogue Location)

View Mode: Unknown Radio Location Estimation

Unknown Radios: 00-13-46-16-a0-e0

Transmit Power Assumption (At least one should be selected)

☑ 1 mW ☑ 5 mW ☑ 20 mW ☑ 50 mW ☑ 100 mW

☑ Use Exclusion Algorithm

Probability of Unknown Radio Location

0 - 10 %	10 - 20 %
20 - 30 %	30 - 40 %
40 - 50 %	50 - 60 %
60 - 70 %	70 - 80 %
80 - 90 %	90 - 100 %

Connected to: airoman.aps.anl.gov

Edit Locations: Disabled, Distance Measure Tool: Off

Cyber Security

- Firewalls
- Anti-Spam
- URL filtering
- Network blocking

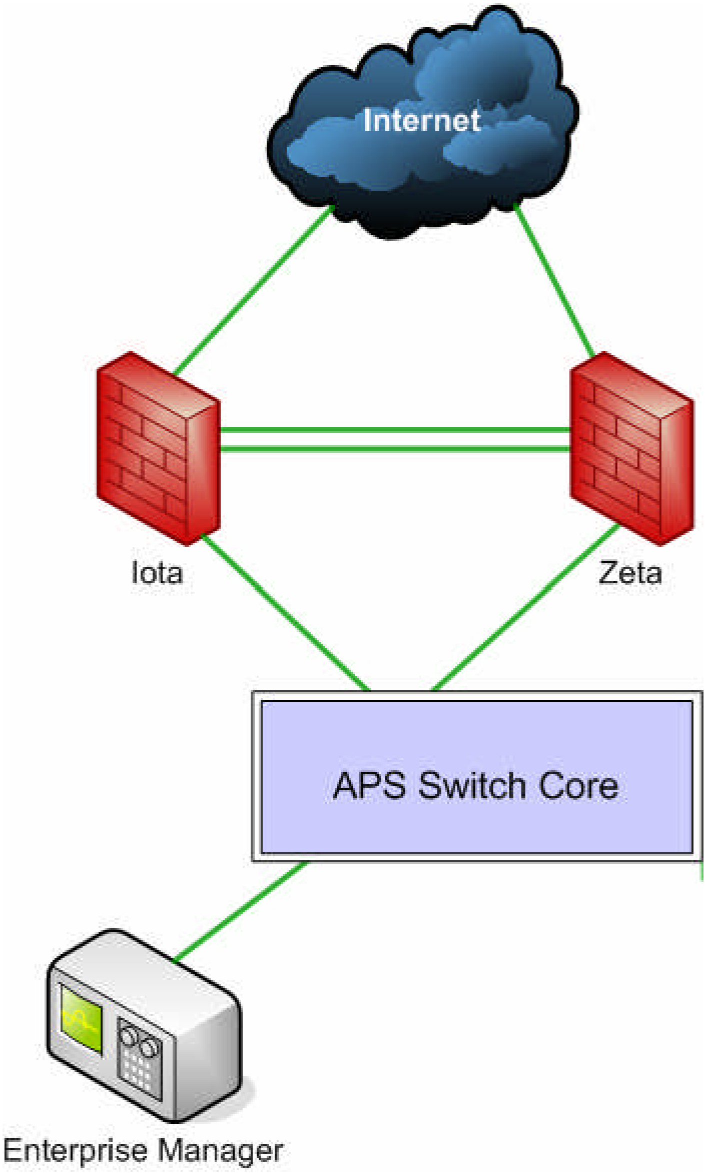
Cyber Security Tier 1 and Tier 2 Firewalls - Defense in Depth

- Tier 1 - Cisco FWSM
  - High availability/reliability
  - Layer 3 only protection - minimal security
  - Visitor/Wireless - permit only outbound communication
  - Protects Tier 2 firewall from attacks on common protocols
  - Efficient for adding shuns/blocks to network

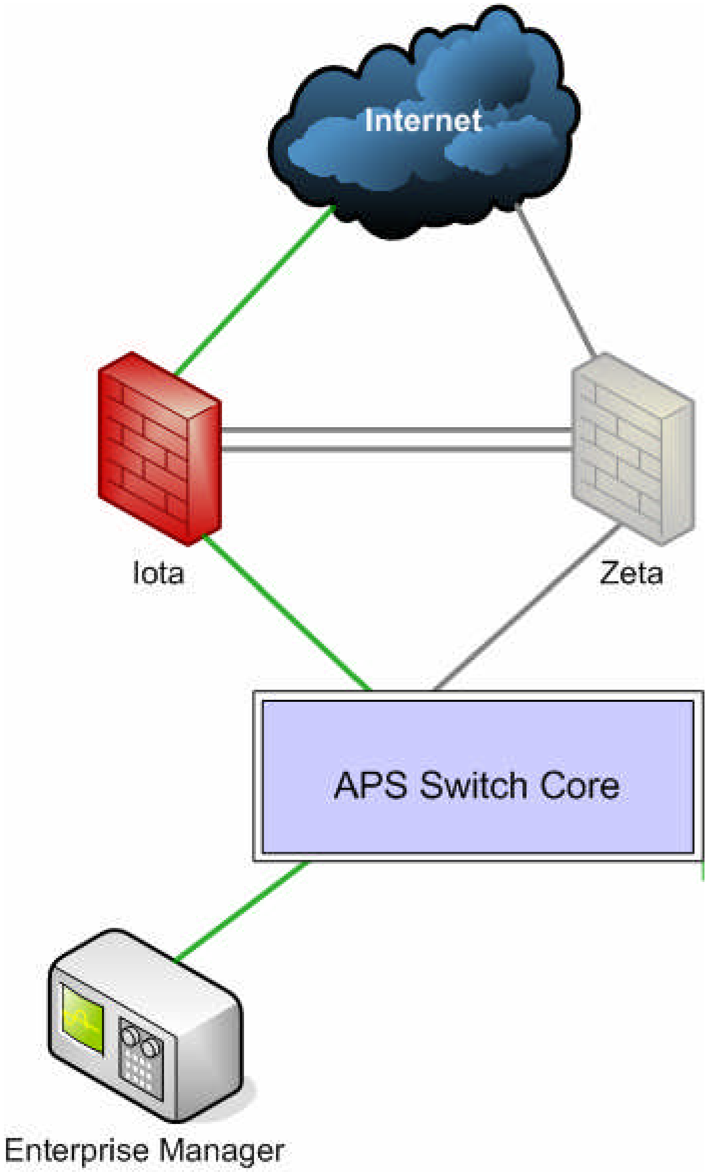
Cyber Security Tier 1 and Tier 2 Firewalls - Defense in Depth continued

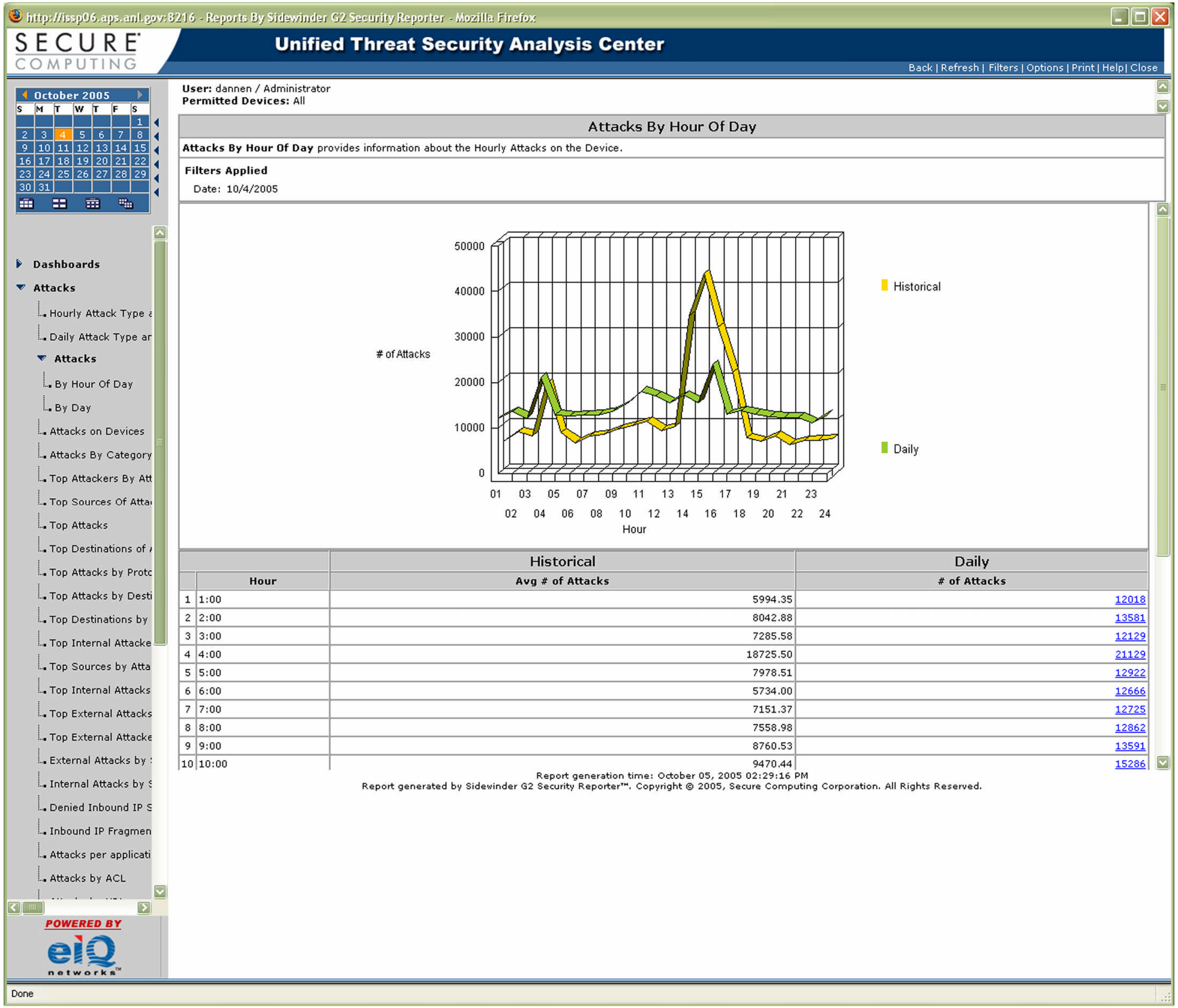
- Tier 2 - Secure Computing SideWinder G2
  - Most comprehensive gateway security appliance in the world
  - Only firewall that has never had a CERT advisory posted against it in over 10 years
  - Same firewall used by military, CIA, FBI and NSA
  - Layer 3 through Layer 7 protection
  - Protocol anomaly detection; traffic anomaly protection
  - Embedded anti-spam and anti-virus engines
  - Smartfilter URL Filtering
  - SecureOS operating system with patented Type Enforcement technology
  - HA Pair fully redundant hardware and network connections
  - Patches install with little or no down time
  - Protection both inbound and outbound
  - Central firewall management

Active-Active Pair



Active-Active Pair





User: dannen / Administrator
Permitted Devices: All

Attacks By Hour Of Day

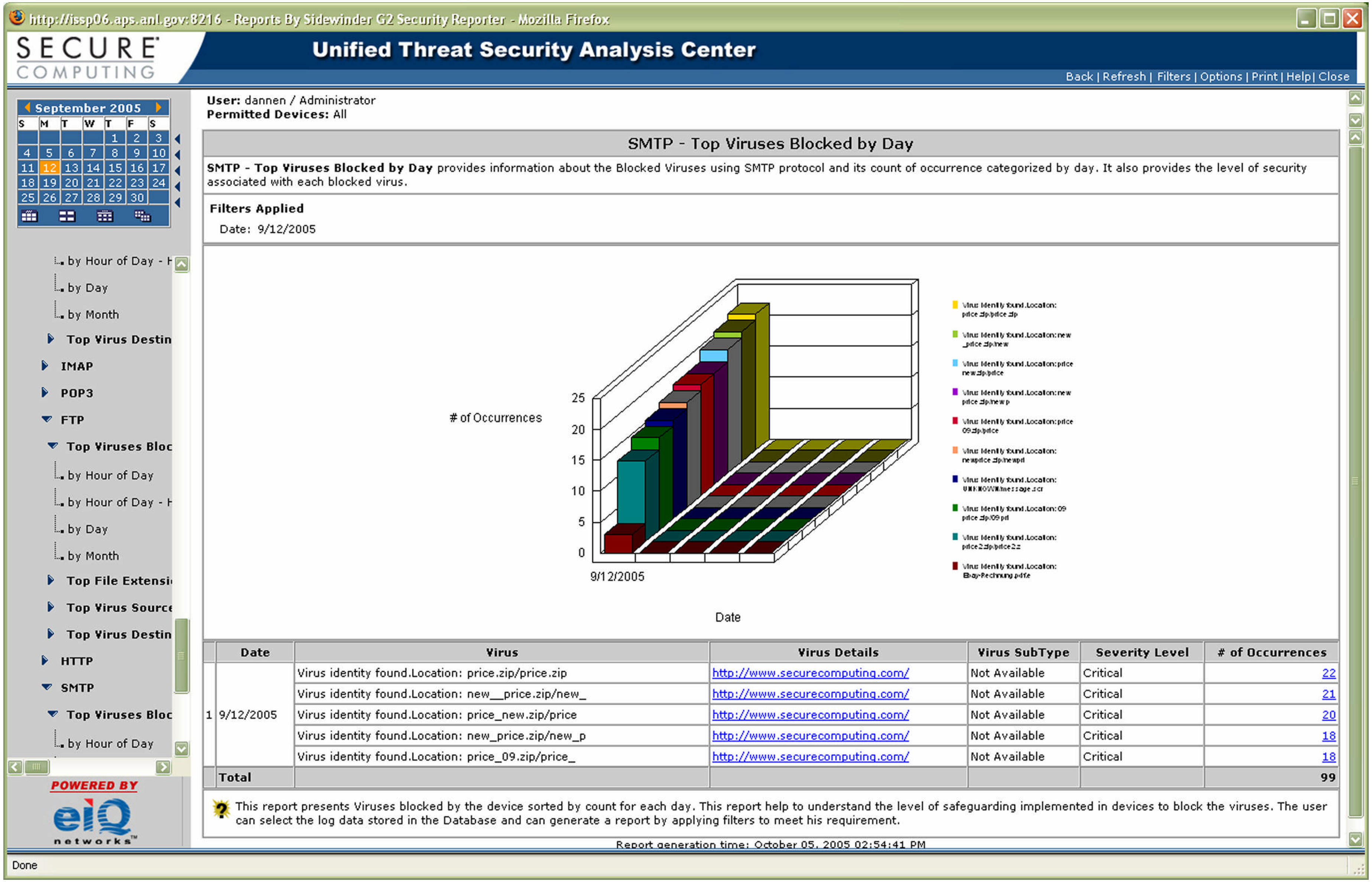
Attacks By Hour Of Day provides information about the Hourly Attacks on the Device.

Filters Applied

Date: 10/4/2005

		Historical	Daily
	Hour	**Avg # of Attacks**	**# of Attacks**
1	1:00	5994.35	12018
2	2:00	8042.88	13581
3	3:00	7285.58	12129
4	4:00	18725.50	21129
5	5:00	7978.51	12922
6	6:00	5734.00	12666
7	7:00	7151.37	12725
8	8:00	7558.98	12862
9	9:00	8760.53	13591
10	10:00	9470.44	15286

Report generation time: October 05, 2005 02:29:16 PM
Report generated by Sidewinder G2 Security Reporter™. Copyright © 2005, Secure Computing Corporation. All Rights Reserved.


http://issp06.aps.anl.gov:8216 - Reports By Sidewinder G2 Security Reporter - Mozilla Firefox
SECURE COMPUTING
Unified Threat Security Analysis Center
Back | Refresh | Filters | Options | Print | Help | Close
September 2005
S M T W T F S
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30
by Hour of Day - H
by Day
by Month
Top Virus Destin
IMAP
POP3
FTP
Top Viruses Bloc
by Hour of Day
by Hour of Day - H
by Day
by Month
Top File Extensi
Top Virus Source
Top Virus Destin
HTTP
SMTP
Top Viruses Bloc
by Hour of Day
POWERED BY
eiQ networks
# of Occurrences
0
5
10
15
20
25
9/12/2005
Date
Virus identity found.Location: price.zip/price.zip
Virus identity found.Location: new_price.zip/new
Virus identity found.Location: price new.zip/price
Virus identity found.Location: new price.zip/new p
Virus identity found.Location: price 09.zip/price
Virus identity found.Location: newprice.zip/newpri
Virus identity found.Location: UNKNOWN/message.scr
Virus identity found.Location: 09 price.zip/09 pri
Virus identity found.Location: price2.zip/price2.z
Virus identity found.Location: Ebay-Rechnung.pdf.e
Done

User: dannen / Administrator
Permitted Devices: All

SMTP - Top Viruses Blocked by Day

SMTP - Top Viruses Blocked by Day provides information about the Blocked Viruses using SMTP protocol and its count of occurrence categorized by day. It also provides the level of security associated with each blocked virus.

Filters Applied

Date: 9/12/2005

	Date	Virus	Virus Details	Virus SubType	Severity Level	# of Occurrences
1	9/12/2005	Virus identity found.Location: price.zip/price.zip	http://www.securecomputing.com/	Not Available	Critical	22
		Virus identity found.Location: new__price.zip/new_	http://www.securecomputing.com/	Not Available	Critical	21
		Virus identity found.Location: price_new.zip/price	http://www.securecomputing.com/	Not Available	Critical	20
		Virus identity found.Location: new_price.zip/new_p	http://www.securecomputing.com/	Not Available	Critical	18
		Virus identity found.Location: price_09.zip/price_	http://www.securecomputing.com/	Not Available	Critical	18
	Total					99

This report presents Viruses blocked by the device sorted by count for each day. This report help to understand the level of safeguarding implemented in devices to block the viruses. The user can select the log data stored in the Database and can generate a report by applying filters to meet his requirement.

Report generation time: October 05, 2005 02:54:41 PM

Tier 3 Firewall for CATs

- Beamline routers have ACLs to protect Beamlines from infecting one another.
- Each Beamline has their own list of rules.
- Logs are reviewed daily for intrusion attempts.

Web URL Filtering

- Smartfilter from Secure Computing built into SideWinder firewall.
- Best web coverage and protection in the industry.
- Provides database of millions of blockable web sites in over 70 categories.
- Blocks Spyware and Phishing web sites.
- Increase productivity and preserve bandwidth for business-related activities.
- SmartReporter provides real time reports of web activity.

Automated Network Blocking

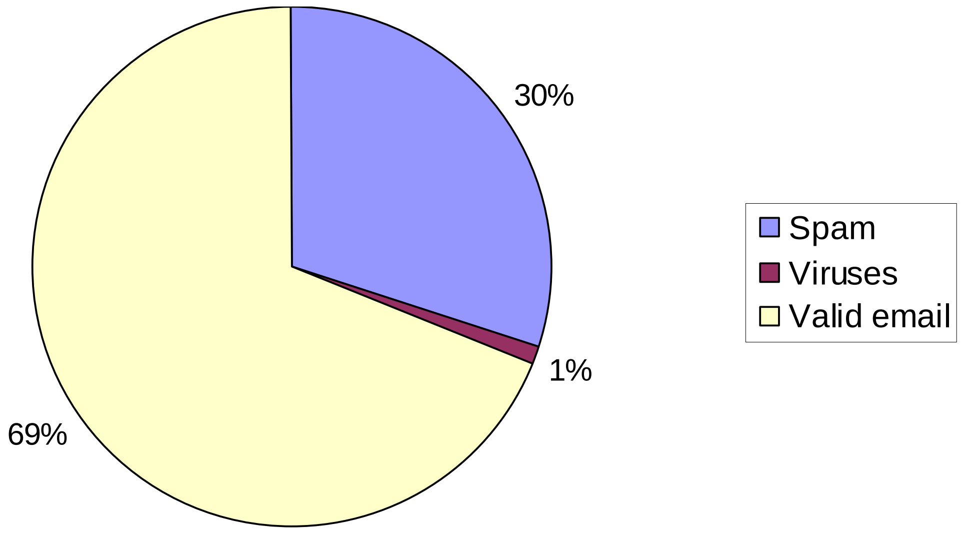
- IT scripts scan firewall and switch data logs looking for suspicious network activity.
- Intrusion Detection System monitors network traffic looking for known virus signatures.
- Blocks are then added automatically to protect our network from intrusion.
- Beamline CSPRs are notified immediately via email when blocks are added.
- 100-400 network blocks are issued each day.

Anti Spam

- Email is scanned using two different spam detection programs.
- Customized spam filter rules are added daily by IT.
- Spam logs are reviewed three times a day for false positives.

Mail Stats

- APS processes between 15,000 and 20,000 emails a day.
- 20% to 30% of all email is detected as spam, 3000-5000 emails.
- Anti-virus signatures are updated hourly.
- Virus infected email varies from 50 to 200 a day.



IT Networking Challenges

- Interrupt driven
  - Daily hacker intrusion attempts
  - Resolve network problems that occurred overnight
  - Walk-ins, phone calls and help desk cases
  - Assist members of IT group to resolve problems
- Who do we serve first?
- How long should a user wait without network connectivity?
- Enhancements, upgrades and new services are very difficult to complete with limited manpower.
- Daily network monitoring and user assistance is delayed to complete these tasks.